View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Schulich Scholars (Schulich School of Law, Dalhousie University)

Canadian Journal of Law and Technology

Volume 9
Number 1 *1 & 2*

Article 6

6-1-2011

Location-Based Services and Privacy

Teresa Scassa

Anca Sattler

Follow this and additional works at: https://digitalcommons.schulichlaw.dal.ca/cjlt

 Part of the Computer Law Commons, Intellectual Property Law Commons, Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation

Teresa Scassa and Anca Sattler, "Location-Based Services and Privacy" (2011) 9:1 CJLT.

This Article is brought to you for free and open access by the Journals at Schulich Law Scholars. It has been accepted for inclusion in Canadian Journal of Law and Technology by an authorized editor of Schulich Law Scholars. For more information, please contact hannah.steeves@dal.ca.

Location-Based Services and Privacy

Teresa Scassa and Anca Sattler[*]

INTRODUCTION

The last decade has seen a rapid growth in the number and variety of location-based services that are available to consumers. While some of the older location-based services are tools such as GPS and other navigation systems, more recent innovations include applications that permit users to call up a variety of different information about their current locations, such as the nearest Italian restaurant, or the best deals at a favourite store. Location-based services (LBS) also allow individuals to share their location with friends in a wide range of social networking contexts. Location-based services are already shifting from pull to push applications. Information can now be pushed automatically to users based on their location. The options for such services are virtually limitless, and include mobile-marketing, public transportation applications, information about local points of interest, health care applications connected to remote treatment systems, or tools to find the closest election-day polling booth.

There is no doubt that many location-based services offer real benefits to users. Yet location-based services raise inevitable user privacy concerns. These concerns operate on multiple levels and involve many players. In some applications, privacy issues will arise between individual users, where, for example, applications permit the tracking of movements of family members, co-workers or "friends".[1] Location-based services may also result in the collection of a new layer of personal information about consumers by private sector companies. Information about individuals and their movements has meaningful commercial value, and the potential for the collection, use and disclosure of this information is significant.[2]

---

[*] Teresa Scassa is Canada Research Chair in Information Law and Professor, University of Ottawa, Faculty of Law, Common Law Section. Anca Sattler is a third year student at the University of Ottawa, Faculty of Law, Common Law section. This paper is part of a broader research project generously supported by the GEOIDE Network. Thank you to Charles Sanders for reading and commenting on an earlier draft of this paper.

1 Examples of location-based services which permit the sharing of location information with "friends" include Google Latitude (http://www.google.com/intl/en_us/latitude/intro.html) and Facebook Places (http://www.facebook.com/places/). Cell phone location data can also be used to track the movements of the cell phone user, for example tracking a teen (http://www.gpsfortoday.com/gps-tracking-for-teens/) or secretly tracking a spouse or an employee (http://www.whereareyougps.com/).

2 John B. Morris Jr., "The Privacy Implications of Commercial Location-Based Services" (Statement before the House Committee on Energy and Commerce, 24 February 2010) at 6, online: Center for Democracy and Technology [CDT] <http://www.cdt.org/files/pdfs/CDT-MorrisLocationTestimony.pdf>. Morris notes that "the number of possible uses for location data is ever-growing and the number of companies handling location information is continuously expanding as well:

Location-based services also raise the spectre of state surveillance of individual activity — either concurrent with an individual's movements (tracking), or retrospectively, through searching records of individual patterns of movement.[3] These are just some of the contexts in which privacy issues are raised.

In this paper we begin by describing location-based services, their evolution and their future directions. We then outline privacy issues raised by such services. In Part III we consider how current Canadian data protection laws apply to location-based services, and indicate where such laws fall short of addressing the full range of issues raised by location-based services. Part IV of the paper explores some technological methods to address the privacy challenges raised by location-based services. The paper concludes with a series of recommendations.

I. LOCATION-BASED SERVICES

Location-based services are proliferating largely due to the dramatic rise in the number of GPS-equipped mobile devices used by consumers. Such devices include smart phones, tablet computers and hand held Global Positioning Systems (GPS). Newer versions of internet browsers are also "location aware", facilitating the use of location information in tailoring the user's web experience.[4] Location-based services are premised on the sharing of a user's location information with a set of specified individuals within their circle of family, friends or associates. Services such as Google Latitude,[5] Glympse,[6] Foursquare[7] or Gowalla,[8] enable this kind of location sharing. Location-sharing can also have a non-consensual dimension. For example, it can be used by employers to track the location of their employees,[9] or

---

handset vendors, operating system vendors, advertisers, advertising networks, and analytics companies may also have access to precise, sensitive information about where users are located".

3 Cases in both the U.S. and Canada have involved law enforcement access to location information in the hands of third party service providers. See, e.g.: *R v. Plant*, [1993] 3 SCR 281 [*Plant*]; *R v. Gomboc*, 2010 SCC 55, [2010] 3 SCR 211 [*Gomboc*]; *Smith v. Maryland* (1979), 442 U.S. 735 (U.S. Md.) [*Smith*]; *In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 534 F Supp 2d 585 (WD Pa 2008). These cases are discussed in greater detail below. Civil liberties groups have expressed concerns about the ease with which law enforcement agencies might access this data without a warrant. See CDT, *supra* note 2 at 3.

4 See, for example, Mozilla Firefox, Location-Aware Browsing, online: <http://www.mozilla.com/en-GB/firefox/geolocation/>; Google, Google Chrome Becomes Location Aware, online: <http://google-chrome-browser.com/google-chrome-becomes-location-aware>.

5 Google Latitude: <http://www.google.com/intl/en_us/latitude/intro.html>.

6 Glympse: <http://www.glympse.com/>.

7 Foursquare: <https://foursquare.com/>.

8 Gowalla: <http://gowalla.com/>.

9 National Work Rights Institute, "On Your Tracks: GPS Tracking in the Workplace" (2010) at 10–15, online: <http://workrights.us/wp-content/uploads/2011/02/NWI_GPS_Report.pdf>.

by parents to track the location of their children, with or without their knowledge or consent.[10] In all cases, however, location information is explicitly shared with a specified list of individuals.

Mobile marketing is a growing location-based activity in which location information is used. There is also an ever-growing and ever-changing group of services that can be delivered to individuals based on their location. For example, users searching for a particular clothing chain's web site might be asked for their location information in order to provide them with more specific information about outlets near them.[11] Using location-based services, individuals may request information about nearby tourist attractions, or the location of other services or institutions. They may also be provided emergency and other assistance based on their location.[12] Public transit information may also be delivered in this way.[13] Other types of location-based services have emerged including those which augment the information delivered,[14] or those which combine geo-location with games.[15]

(a) Determining a Mobile Device's Location

Location-based services rely upon information about a user's location. This information is typically gathered and communicated by mobile devices which users

---

10 Multiple services exist to turn GPS-enabled cell phones into tracking devices. Many of these cite the virtues of being able to track family members. See, for example: <http://www.accutracking.com/> or <http://www.whereareyougps.com/>.

11 Location aware browsing is available with Mozilla Firefox 3.5 and higher <http://www.mozilla.com/en-GB/firefox/geolocation/>; Google Chrome <http://google-chrome-browser.com/google-chrome-becomes-location-aware>; and Internet Explorer 9 <http://windows.microsoft.com/en-US/internet-explorer/products/ie-9/windows-internet-explorer-9-privacy-statement>. These three most popular browsers prompt users when a website is requesting their location information, and the user is given the option to share or not. Location aware browsing is turned on by default in Bing. For a discussion of the collection of location information from web browsers, see Amir Efrati & Jennifer Valentino-Devries, "Computers, Too, Can Give Away Location", *The Wall Street Journal* (27 April 2011) online: <http://online.wsj.com/article/SB10001424052748703778104576287401134790790.html>.

12 An example of this is the OnStar service which provides emergency and other support services based on the vehicle's location. See online: <http://www.onstar.com/web/portal/home>.

13 For example, the NextBus system offers transit arrival time predictions based on data gathered from GPS equipped vehicles, online: <http://www.nextbus.com/corporate/index.htm>.

14 Poynt offers a local search application with "augmented reality features" that allow users to locate restaurants, shops or other features in their vicinity and then to obtain layers of additional information. See online: <http://www.poynt.com>.

15 An early location-based game experience was offered by Geocaching, a form of GPS-enabled treasure hunting <http://www.geocaching.com/>. More recent initiatives include Foursquare, which allows users to earn points by checking-in to places, and to win badges for discovering new features. See also: Maria Ebling & Ramón Cáceres, "Gaming and Augmented Reality Come to Location-Based Services", *IEEE CS* (2010) online: <http://csdl2.computer.org/comp/mags/pc/2010/01/mpc2010010005.pdf>.

carry with them, or are situated in a vehicle driven by the user. The ability to communicate information about their location is generally crucial to the proper functioning of a device. For example, a mobile phone cannot send or receive calls without communicating information about its location on an ongoing basis.

Depending on the technology used, there are different ways in which a device's location can be determined. One way to determine a device's location relies upon network infrastructure and different positioning technologies (such as Wimax,[16] Wi-Fi,[17] UWB,[18] and RFID).[19] This method is used with mobile devices without a built-in GPS, where the device's position is estimated relative to base, or beacon nodes.[20] The process begins by estimating the distance and angle between the device and multiple beacon nodes in its vicinity, either by the device itself, or by the network service. The device's position is then calculated by applying one or more of the fundamental geometric principles of *trilateration*, *multilateration* and *triangulation*.[21] Distance can be calculated by studying the signals received. When the user of the device is in motion, the direction of movement can be determined by the angle of signal received, or by making use of motion sensors such as accelerometers.[22]

Trilateration is a technique used to determine the position of a point, or a mobile device in this case, based on a calculation of the point's distance from three or more known locations. This method can be contrasted with *triangulation*, which involves the measurement of angles from the device's location to three or more beacons with known or fixed locations. Locating an object by *multilateration*[23] entails the computation of the time difference of arrival of a signal emitted from that object to three or more receivers. One or a combination of these methods can be used in identifying the device's location.

Another method of determining the location of a mobile device is through the

16 WiMAX (Worldwide Interoperability for Microwave Access), online: <http://www.techpluto.com/wimax-in-detail/>.

17 Wi-Fi is a trademark of Wi-Fi Alliance. See online: <http://www.wi-fi.org/discover_and_learn.php>.

18 UWB (UltraWide Band) is a radio technology used at low energy levels for short range communications at high bandwidth. See Nicholas Cravotta, "Ultrawideband: The Next Wireless Panacea?", *EDN* (17 October 2002) online: <http://www.edn.com/article/492456-Ultrawideband_the_next_wireless_panacea_.php>.

19 RFID (Radio Frequency Identification). See "What is RFID", *RFID Journal* (2005) online: <http://www.rfidjournal.com/article/articleview/1339/1/129/>.

20 Syed A. Ahson & Mohammad Ilyas, eds, *Location-Based Services Handbook: Applications, Technologies, and Security*, (Boca Raton, FL: CRC Press, 2011) at 3 [LBS Handbook].

21 *Ibid.*

22 Accelerometers are sensors built in mobile devices that can measure the tilt, orientation and motion of a device. See MEMSIC, online: <http://www.memsic.com/products/sensor-components/accelerometers.html>.

23 See online: <http://www.multilateration.com/surveillance/multilateration.html>.

use of GPS,[24] and assisted GPS, a technology used to augment GPS signals. This is useful in urban areas or indoor locations where signals may be weak.[25] A GPS-enabled device can transmit the information captured from satellites through the cellular network to the location server, which then will transmit information back to the mobile device. GPS technology can be combined with other location technologies to produce more accurate location information.[26]

Laser, ultrasound and sound technologies are currently being researched to improve the accuracy and to speed up the process of calculating a device's location.[27] If more than one method is available for determining location, the precision and the quality of service provided by the location-based services are greatly improved. This availability of methods depends largely on the technological capabilities of the device. The current trend is towards ongoing improvements in the accuracy of location information.

Smart phones and other such mobile devices emit location information every few seconds. This process occurs repeatedly so that the device is always aware of its location in relation to communication towers and the user experiences no delays in receiving or transmitting calls. Users may be unaware that this process of communicating location information is rapid, regular and ongoing. It is not initiated solely by the user's choice to make use of the device.[28]

More recently, Wi-Fi access points have been used as a means of determining a device's location.[29] Wi-Fi access points emit their location information in the form of a Media Access Control Address (MAC address) on a continuous basis.[30] Wi-Fi Positioning Systems (WPS) collect and map the location of Wi-Fi access points. When a user uses a mobile device, the device will seek out nearby Wi-Fi access points. The device's location can be calculated based on those access points visible to the device.[31] In the course of this process individual devices may also be

---

24 Global Positioning System (GPS) is a satellite-based navigation system made up of a network of 24 satellites placed into orbit by the U.S. Department of Defense, originally intended for military applications (see online: <http://www8.garmin.com/aboutGPS/>).

25 See Palenius, T. & Wigren, T., "Optimized search window alignment for A-GPS", (2009) 58 No 8 IEEE Trans. Veh. Technol. 4670.

26 Article 29 Data Protection Working Party, *Opinion 13/2011 on Geolocation services on smart mobile devices*, adopted 16 May 2011, 881/11/EN WP 185 at 5 [Working Party 13/2011], online: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf>.

27 LBS Handbook, *supra* note 20 at 68.

28 Charles Arthur, "Android phones record user locations according to research", *The Guardian* (21 April 2011) online: <http://www.guardian.co.uk/technology/2011/apr/21/android-phones-record-user-locations>; Scott Thurm & Yukari Iwatani-Berlin Heidllbergof data. See,er of Canada, Kane, "Your Apps are Watching You", *The Wall Street Journal* (17 December 2010) online: <http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html>.

29 Working Party 13/2011, *supra* note 26 at 5.

30 *Ibid.*

31 Anne Cavoukian & Kim Cameron, "Wi-Fi Positioning Systems: Beware of Unintended Consequences" (Toronto: Office of the Information and Privacy Commissioner of On-

identified by their own unique MAC addresses.[32]

(b) History and Evolution of Location-Based Service Technology

Location-based services were first introduced with Enhanced911 (E-911), an initiative of the US Federal Communications Commission (FCC) to make all wireless phones location-capable. The goal was to enable emergency services to quickly and accurately determine the location of a call placed using a cell phone and to deliver the location information to the closest Public Safety Answering Point.[33] Operators of mobile services began to introduce commercial location-based services in order to gain return for their E-911 investments. These initial developments were characterized by finder services, where information was sent to a user upon request (e.g. finding a restaurant or a tourist attraction).[34] Because of poor design, limited precision and reduced functionality, these services failed to gain in popularity.

Significant changes in location-based service technologies were made possible by the development of low powered GPS-enabled mobile phones and assisted GPS, as well as the introduction of the 3G broadband wireless services.[35] Better location-based services, such as real-time mapping, points-of-interest content or navigation support, could be offered with the advent of new GPS-enabled mobile phones and devices, which support high accuracy positioning.[36] These improvements led to the next generation of location-based services, which facilitated the delivery of mundane services at the push of a button (i.e. calling a taxi to the user's location without dialling a service operator), or allowed a user's location to trigger the sending of information to the mobile device.

One of the reasons why location-based services have gained in popularity is the shift from a *reactive* to a *proactive* system. While a reactive system simply responds to a user's location, a proactive system allows users to register their interests and/or preferences. Based on this information, the proactive system will automatically push relevant content to the user. In a location-based system, this might include notifying users when they are approaching points of interest.[37] These proactive systems require less input from the user, yet deliver a wide range of information. These systems require a constant tracking of the mobile device to enable an

---

tario, June 2011), online: <http://www.ipc.on.ca/images/Resources/wi-fi.pdf>; Working Party 13/2011, *supra* note 26 at 6.

32 Cavoukian & Cameron, *supra* note 31 at 10.

33 Federal Communications Commission News, "FCC Adopts Wireless 911 Rules" (13 May 1999) [FCC], online: <http://www.fcc.gov/Bureaus/Wireless/News_Releases/1999/nrwl9016.html>.

34 M. A. Labrador, K. Michael & A. Kupper, "Advanced location-based services" (2008) University of Wollongong Research Online at 1, online:<http://ro.uow.edu.au/infopapers/584>.

35 Paolo Bellavista, Axel Küpper & Sumi Hela, "Location-Based Services: Back to the Future" (2008) 7:2 Pervasive Computing, IEEE CS 85 at 85.

36 Labrador, *supra* note 34 at 1.

37 Bellavista, *supra* note 35 at 86.

efficient supply of information.[38]

Another recent development is the emergence of cross-referencing services, where the user and the target for information are not always the same. This service takes information from one user in order to serve another.[39] For example, in May 2011, it was reported that TomTom, a manufacturer of portable satellite navigation systems, was selling anonymized data collected from its high-end navigation devices to authorities throughout Europe, U.S. and Canada, to be used for traffic control purposes.[40]

The multifunctional nature of GPS-equipped smart phones adds to the complexity of location information capable of being shared. This includes cell phone camera functions that geo-tag photographs.[41] Accelerometers, a type of sensor that is increasingly common in mobile devices, are capable of measuring acceleration, tilt and orientation, and thus have the potential to increase the fine detail of the location information that is being gathered.[42] Transportation systems can also make use of and gather data from GPS-enabled mobile phones on board vehicles in order to estimate the traffic flow on roads and highways.[43] Location-based services continue to evolve as new technological capabilities become widely available and highly affordable. One example is the availability of location-sensitive billing services, where certain service providers can automatically charge a user when using their service, such as road tolls.[44]

Research is being conducted on applications with augmented reality features, which would enable a mobile phone equipped with a camera, a compass and a GPS

---

38 *Ibid* at 86.

39 *Ibid.*

40 TomTom has admitted and apologized for selling drivers' GPS data to authorities. The Dutch authorities have used the GPS data to build better speed bumps and position speed cameras more efficiently. In Ontario, GPS data acquired from TomTom was used by authorities to optimize evacuation routes for the city of Toronto. See "TomTom Will Tighten Data Sharing Rules", *The Wall Street Journal* (3 May 2011) at 26, online: <http://blogs.wsj.com/tech-europe/2011/05/03/tomtom-will-tighten-data-sharing-rules/>.

41 *Ibid.*

42 *Supra* note 22.

43 See Daniel B. Work et al, "Lagrangian Sensing: Traffic Estimation with Mobile Devices", online: <https://netfiles.uiuc.edu/dbwork/www/pdf/ACC09.pdf>. See also S. Amin et al, "Mobile century-using GPS mobile phones as traffic sensors: a field experiment" in 15th World Congress on ITS (New York, NY: Intelligent Transport Systems, 17–20 November 2008).

44 See Stefan Steiniger, Moritz Neun & Alistair Edwardes, "Foundations of Location-Based Services" University of Zurich at 26, online: Project CartouCHe <http://www.spatial.cs.umn.edu/Courses/Fall07/8715/papers/IM7_steiniger.pdf>. The toll system differs from the already popular RFID chips embedded in vehicles, because this system can calculate the actual distance travelled by the vehicle on the toll highway and can charge the user based on the distance. (See for example Toll-Collect service in Germany, online: <www.toll-collect.de>.) This ensures that traffic flow is not disrupted as vehicles are not required to stop and pay at a booth upon exiting the highway.

to superimpose information about points of interest on a live camera view, based on the phone's current position, orientation and the direction in which the camera is pointing.[45] In its May 16, 2011 report, the EU Data Protection Working Party on Geolocation Services expressed a sense of urgency in addressing data protection in the context of mobile technologies because of the proliferation of mobile devices and the rapid advancement of the technology.[46]

(c) Positive Uses of Location-Based Services

The potential for the development of location-based services is virtually limitless and may extend into every sphere of human endeavour. An obvious benefit brought by location-based services is the ability to filter vast amounts of content available over the Internet, and to deliver to the user only information in which she may have an interest.[47] For example, a simple query for a pharmacy would not return all registered pharmacies for the user to sift through until she finds the pharmacy closest to her location. The location-based service would return information related to only those pharmacies in the user's immediate vicinity.

Location-based services also serve the user by pushing information to her, such as discounts or coupons as she passes by a department store, alerts of risks when entering a high-crime district, or warnings before encountering a traffic jam on the highway.[48] Furthermore, by sharing location information, all users benefit from more current localized information. Mobile devices connected to location-based services can also assist in finding missing persons.

Location awareness may also permit a variety of health and emergency management benefits. For example, the Virtual Blood Bank Project in Delhi, India uses smart phones to build a pervasive network capable of giving users instantaneous information about available blood donors in their vicinity, which may be critical in emergency situations.[49] Other health care applications may include the ability to transmit critical health related information to a hospital along with the patient's location and estimated time of arrival to the emergency room, allowing the hospital

---

45 Metro Paris Subway: <http://www.metroparisiphone.com/index_en.html>.

46 Working Party 13/2011, *supra* note 26.

47 Sidney Shek, "Next-Generation Location-Based Services For Mobile Devices" CSC (February 2010) at 1, online: <http://assets1.csc.com/lef/downloads/CSC_Grant_2010_Next_Generation_Location_Based_Services_for_Mobile_Devices.pdf>.

48 *Ibid.*

49 Indian citizens register as donors or recipients on Web sites created for these purposes. They specify their blood type and contact information. A server matches the blood type needed and the location by a recipient with the donors in close proximity, and sends this information to the recipient. Concerns have been raised about the disclosure of personal information about the donors. See Muhammad Sajidur Rahman et al, "Smart Blood Query: A Novel Mobile Phone Based Privacy-aware Blood Donor Recruitment and Management System for Developing Regions", Advanced Information Networking and Applications (AINA), 2011 IEEE Workshops of International Conference (22–25 March 2011) at 544–548.

to make all necessary preparations before the patient's arrival.[50]

II. PRIVACY CONCERNS AND RISKS

There is no doubt that the explosive development of location-based applications presents a whole new series of privacy concerns and risks for its users. The use of GPS-enabled hand-held devices has become ubiquitous. Such devices include smart phones, PDAs, and tablet computers. In this section we first discuss consumer attitudes towards geolocation privacy before providing an overview of some of the privacy concerns raised by the use of these technologies.

All identified risks involve the fact that either the location information itself, or a combination of location information with other information, has the potential to reveal excessive amounts of personally identifiable information about individuals. As noted by the EU Data Protection Working Party in its recent opinion on geolocation services, "[a]ll kinds of information can be connected to a geographic location, such as financial data, health data and other consumer behavioural data."[51] This information can include details that the individual had no intention of sharing. The phenomenon of data profiling adds to the privacy risk, as it is increasingly the case that personal information from a wide variety of sources is combined in profiles of a disturbing level of detail.[52]

(a) Concerns and Consumer Attitudes

Canadians are fairly careful about sharing their location information. A 2009 survey commissioned by the Office of the Privacy Commissioner of Canada[53] found that 90 per cent of Canadians are concerned about the impact new technology has upon their lives.[54] The same report indicates that an overall majority of Canadians (98%) find strong privacy laws to be important. Although Canadians may not be aware of all privacy risks associated with revealing their location information, the EKOS study found that Canadians tend to have high expectations of

---

50 See Ahn, J. et al, "A Study on the Application of Patient Location Data for Ubiquitous Healthcare System based on LBS" (2008) IEEE 10th International Conference on Advanced Communication Technology at 2140–2143, online: <http://www.iaeng.org/publication/WCE2008/WCE2008_pp270-273.pdf>.

51 Working Party 13/2011, *supra* note 26 at 3.

52 See, e.g., Jason Millar, "Core Privacy: A Problem for Predictive Data Mining" in Ian Kerr et al, eds, *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Oxford: Oxford University Press, 2009) at 103.

53 EKOS Research Associates Inc. Canadians and Privacy, Final Report (March 2009) online: <http://www.priv.gc.ca/information/survey/2009/ekos_2009_01_e.cfm#sec1>.

54 Office of the Privacy Commissioner of Canada, "DRAFT: Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting and Cloud Computing" online: <http://www.priv.gc.ca/resource/consultations/report_2010_e.pdf>. Numerous mobile device applications entice users to disclose their location information without much concern for privacy, even when such information is not needed to perform the service. See John Krumm, "A Survey of Computational Location Privacy" (Redmond, WA; Microsoft Research, 2009) at 392 [Krumm].

privacy. This extends to online activities. They worry about disclosing too much information, especially if data is shared with services outside of Canada.[55] The FTC in the U.S. has similarly observed that "notwithstanding consumers' lack of understanding about how companies collect and use consumer data, consumers care about their privacy."[56]

The FTC Privacy Framework document identifies consumer awareness as a key factor in dealing with privacy issues. In other words, where consumers are aware of privacy risks, and of effective means to address them, they will take such steps.[57] However the investment of time and effort required of consumers in order to protect their privacy may dampen their willingness to take these steps.[58] This suggests that clear and accessible information, as well as effective and efficient privacy tools are important components of appropriate privacy protection. In the Canadian context this may mean that data protection laws should be interpreted so as to place a greater onus on companies to ensure that privacy policies and privacy options are made available to consumers in accessible and user-friendly ways.[59]

The context in which location information is requested is directly connected with the users' willingness to share their location information.[60] Canadians are less comfortable sharing their location information when their location is being disclosed in real-time, and when they have no control over who has access to this information.[61] A Natural Resources Canada survey on privacy and the use of geospatial information found that approximately half of respondents could not see any benefits provided by location-tracking technology.[62] The same survey indicated that respondents were most comfortable with location tracking where they perceived a compelling benefit such as personal safety or improved emergency services.[63]

An ever-increasing number of children and teenagers use mobile devices capable of gathering and sharing location information. Individuals belonging to this age category seem least concerned with risks associated with disclosure of such infor-

---

55 *Ibid.*

56 The U.S. Federal Trade Commission (FTC), *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policy Makers*, Preliminary FTC Staff Report, (December 2010) at 28 [Preliminary FTC Report] online: <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>.

57 *Ibid.*

58 *Ibid.*

59 For example, in PIPEDA Case Summary #2009-010, [2009] CPCSF No 10, the Assistant Privacy Commissioner found that where the relevant information had to be culled from FAQs, the service agreement and a web page providing network management information, notice to consumers was not sufficiently transparent to meet the requirements of the law.

60 *Research related to privacy and the use of geospatial information*, Natural Resources Canada (November 2009) at ii, online: <http://epe.lac-bac.gc.ca/100/200/301/pwgsc-tpsgc/poref/natural_resources/2009/091-08/report.pdf>.

61 *Ibid.*

62 *Ibid.*

63 *Ibid* at 56.

mation and they may not be fully aware of the implications and consequences of their actions.[64] The Federal Trade Commission in the United States recognized the weakness of the *Children's Online Privacy Protection Act* (COPPA)[65] in contexts where teenagers provide inaccurate information about their age in order to obtain access to otherwise restricted online services. For example, a recent study showed that millions of Facebook users were under the age of 13.[66]

(b) Risks

There are several privacy risks associated with the use of location-enabled devices and location-based services. In this section, we discuss and highlight some of these risks. We divide these into three categories: information-sharing by users, data profiling, and information sharing with law enforcement.

(i) Information Sharing by Users

Many applications now exist which permit users to share their location with others.[67] Typically, these "others" are selected by the person who chooses to disclose his or her information. For example, a user might identify certain friends or family members who can access her location information. However, in some cases, this ability to choose may be overridden by default settings.[68] For example, Facebook's "Places" application will automatically share one's location information with all of one's friends after one has checked-in to a place unless this feature is turned off by the user.[69] Given that many people have a large number of "friends", a general default of this nature raises the risk that location information

64 "Protecting Youths in an Online World", Hearing Before the Subcommittee on Consumer Protection, Product Safety, and Insurance Committee On Commerce, Science, And Transportation United States Senate, 111th Cong. (15 July 2010) online: <http://www.ftc.gov/os/testimony/100715toopatestimony.pdf>.

65 *Children's Online Privacy Protection Act of 1998*, 15 USC §6501-6506 (1998), Pub L No 105-277, [COPPA].

66 Wailin Wong, "Millions of underage kids use Facebook, Consumer Reports says", *Chicago Tribune* (10 May 2011) online: <http://www.chicagotribune.com/business/breaking/chibrkbus-millions-of-kids-under-age-13-use-facebook-consumer-reports-says-20110509,0,4123052.story>.

67 Popular examples include Google Latitude, Foursquare, Facebook Places, and Gowalla. *Supra* notes 5, 7 and 8.

68 Facebook claims that, for "most people", check-ins are set by default to share location information with the user's Facebook friends only. A video (https://www.facebook.com/video/video.php?v=10150265360030484) released by Facebook in connection with default sharing with "Places", explains how person A can be tagged by another person B using Places, thus immediately revealing person A's whereabouts. Another default sharing set to "enabled" is for "Friends can check me into places". Therefore, if person A is not aware of person B using Facebook Places and she did not change her default Facebook settings, person A's location information can become public unbeknownst to her.

69 For more information and related sites see Facebook Places and Privacy" EPIC.org, online: <http://epic.org/privacy/facebook/places/>.

will be inadvertently disclosed to persons with whom one would prefer not to share. Similarly, Foursquare, the popular location-based social networking site, defaults to sharing the location and time of each of the user's check-ins with "friends" and with the Foursquare website. Through its "who's here" feature, it goes a step further, defaulting to share the information of users in that specific location with anybody, not just with friends.[70] The disclosure of location information to a broad range of persons without the awareness of the data subject creates a range of different privacy risks. Not only do individuals become vulnerable to stalking or other unsought contact, but the location information may result in information about sensitive activities (visits to medical clinics or political gatherings, for example) being inadvertently shared with others.[71] Location-sharing by minors raises its own serious privacy and security concerns.

The ability to control who may access one's location information is often touted as a privacy protective feature. However, even where a user is aware of and exercises these controls there may still be risks. These include the risk that a "friend" will share the user's location information with someone who the user does not wish to have it (such as an ex-lover, for example). Information may also fall into the hands of others when a device is lost, loaned or stolen. Further, not all uses of location features are necessarily consensual. There have been concerns raised about employers who provide employees with location-enabled smart phones or other devices without informing the employee that tracking features are enabled.[72] When families share cell phone plans, the main subscriber may be able to access location information relating to all other phones in the plan.[73] Concerns have been repeatedly raised about the risks posed by location-enabled devices to women seeking to leave abusive partners.[74] Recent news reports indicate that the iPhone 4 backed up and stored detailed location information on users' computer hard-drives

70 See Foursquare sharing default settings, online: <http://foursquare.com/privacy/grid>.

71 Working Party 13/2011, *supra* note 26 at 7.

72 National Work Rights Institute, "On Your Tracks: GPS Tracking in the Workplace", (2010) online: <http://workrights.us/wp-content/uploads/2011/02/NWI_GPS_Report.pdf>. Parents can also use similar features to track their children with or without the child's knowledge.

73 Annys Shin, "Maryland family helps to catch a thief using cell phone's GPS technology", *The Washington Post* (27 October 2010) online: <http://www.washingtonpost.com/wp-dyn/content/article/201010/27/AR2010102708080.html?hpid=topnews>. Services such as Sprint Family Locator, for example, explicitly permit subscribers to sign up to track the location of family members; see online: <https://sfl.sprintpcs.com/finder-sprint-family/signIn.htm>.

74 See, e.g., Justin Scheck, "Stalkers Exploit Cellphone GPS", *Wall Street Journal* (3 August 2010) online: <http://online.wsj.com/article/SB10001424052748703467304575383522318244234.html>; Andrew Wentzell, "Cell Phone Tracking: The Use of GPS Technology in Stalking" (November 2010) 3:2 Domestic Violence Review, online: <http://www.flcourts.org/gen_public/family/bin/Domestic%20Violence%20Review%20Vol%20III%20Issue%201.pdf>.

without notice or consent.[75] This data would be available to anyone who had access to the computer or device and who knew where to look.

Even in cases where users consent to a certain amount of information sharing, they may have an imperfect sense of how an analysis of such data might be used to draw certain inferences. In some cases, location information may be shared inadvertently. Users may simply forget that they have enabled the sharing of location information, or they may be unaware that such information is being shared. Not all users of digital camera equipment, for example, are aware that photographs they take may contain geo-referenced information.[76] It has been demonstrated that individuals who post geo-tagged photographs or other geo-referenced information may permit inferences to be drawn about the location of their home or workplace.[77]

The use of location-enabled devices, such as smart phones and tablet computers may also result in the collection, use and disclosure of location information for purposes not directly related to the delivery of any particular location-based service. For example, in April 2011, Apple Computers became embroiled in controversy after reports surfaced that the iPhone 4 collects and stores detailed location information about users on their phones and other devices synched with the phone.[78] While the location information may have been necessary to deliver mobile communication services, the longer term storage of the information was not necessary to the provision of the service. Issues have also arisen with respect to applications that have no location-based functions (for example, simple games for handheld devices), but that nevertheless harvest location information from the mobile device to which they are downloaded.[79]

---

75 Charles Arthur, "iPhone 4 keeps record of everywhere you go", *The Guardian* (20 April 2011) online: <http://www.guardian.co.uk/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears> [Arthur "iphone"].

76 Privacy Rights Clearinghouse, "Geotag, You're It! What your Smartphone might be saying behind your back" (18 October 2010) online: <http://www.privacyrights.org/geotagging-privacy>. The web site "I Can Stalk You" offers consumers help in how to protect their privacy through controlling geotagging; see online: <http://icanstalku.com/>.

77 Kazuhiro Minami & Nikita Borisov, "Protecting Location Privacy against Inference Attacks" (2010) WPES '10 Proceedings of the 9th annual ACM workshop on Privacy in the electronic society; A. Gallagher et al, "Geo-location inference from image content and user tags", 2009 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops. For more scenarios raising privacy concern see G. Friedland & R. Sommer, "Cybercasing the Joint: On the Privacy Implications of Geo-Tagging" Proceedings of the Fifth USENIX Workshop on Hot Topics in Security, (Washington, D.C., August 2010) online: <http://www.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf> at 4 [Friendland].

78 Arthur "iphone", *supra* note 75.

79 "Smartphone apps harvest, spread personal information", *Science Newsline* (29 September 2010) online: <http://www.sciencenewsline.com/technology/2010092912000036.html>. The Center for Democracy and Technology (CDT, *supra* note 2) notes that as of July 2009 there were 3300 location-based apps available at app stores for mobile devices. See also Thurm & Kane, *supra* note 28.

(ii) Data Profiling

The EU Working Party on geolocation services noted that mobile devices tend to be very closely associated with specific individuals. Thus the location information collected and/or shared via such devices can be highly revelatory of those individuals' movements and activities.[80] The information will also reveal patterns of activity and inactivity, permitting further inferences to be drawn.[81] For example, the information might reveal that they spend more time than they should in bars, or that they have made frequent visits to a clinic or hospital. The report notes that "[t]his allows the provider of geolocation-based services to gain an intimate overview of habits and patterns of the owner of such a device and build extensive profiles."[82]

The providers of location-based services or related services (such as the mobile device itself or the telecommunications service provider) are often in a position to track or record the movements of their users with high spatial and temporal fidelity.[83] As a result they may generate a complete history of each user's movements, including the type of location-based services they accessed and the time of access.[84] The fact that records with this kind of detail can be created does not mean that they necessarily will be. However, it is clear that fine-grained personal information of this kind has a commercial value.[85] There is also a track record of companies retaining information for as long as possible with a view to potential future commercial exploitation of the information.[86]

One of the ways in which such information may be exploited is through data profiling. Data profiling of consumers is already a major industry,[87] and there is no doubt that the more detailed and fine-grained the data, the greater will be its commercial utility. Information about location, movements, patterns of activity and so forth could be valuable components of any data profile.[88] Further, information can be inferred about a person based on their patterns of movement even when they act anonymously.[89] A location-based service can build a chronological record over time based on the data transmitted, thus enabling a link from the records to the

---

80 Working Party 13/2011, *supra* note 26 at 7.

81 *Ibid.*

82 *Ibid.*

83 Shek, *supra* note 47. See also Arthur "iphone", *supra* note 75 for recent developments regarding Apple iPhone 4.

84 Egemen Tanin, Rui Zhang & Lars Kulik, "Spatio-Temporal Database Research at the University of Melbourne" (September 2009) 38:3 SIGMOD Record.

85 Millar, *supra* note 52 at 104-105. The Working Party 13/2011, *supra* note 26 at 7, identifies function creep as one of the privacy risks associated with location information.

86 Daniel J., *The Digital Person: Technology and Privacy in the Information Age*, (New York: New York University Press, 2004) at 22–26.

87 *Ibid* at Chapter 2.

88 Shek, *supra* note 47.

89 Krumm, *supra* note 54.

actual user.[90] Geographic location or place can be a powerful identifier.[91]

(iii) Information-sharing with Law Enforcement

Location information gathered by private sector companies may also raise constitutional privacy concerns where such data is sought by law enforcement or national security officials. Although police typically need warrants to use tracking devices linked to individuals, permissive provisions in the *Criminal Code*[92] and in data protection legislation raise the possibility that such data may be sought from private sector companies without judicial authorization.[93] The greater the volume and detail of such information, the greater is the risk to individuals that this information may be used by authorities to profile, investigate or monitor their activities.

Collectively, the widespread collection, use and disclosure of location information raises significant privacy concerns. The existence of this data will inevitably add additional layers to already existing data profiles. The harms that flow from this form of profiling include discrimination, loss of autonomy, dignity and identity.[94] In addition, the technologies incorporate a kind of self-imposed surveillance wherein each citizen carries around the means by which their activities can be monitored and tracked.

---

90 Hasan, C. S., Ahamed, S. I., & Tanviruzzaman, M., "A Privacy Enhancing Approach for Identity Inference Protection in Location-Based Services" 33rd Annual IEEE International Computer Software and Applications Conference (Seattle, 2009) at 1–10 [Hasan et al]; Claudio Bettini, X. Sean Wang & Sushil Jajodia, "Protecting Privacy Against Location-based Personal Identification" *Secure Data Management*, LNCS 3674 (Springer-Verlag Berlin Heidelberg, 2005) 185 [Bettini, "Protecting Privacy"].

91 See generally, T. Scassa "When is Geographic Information Personal Information?" (2010) 10:2 OUCLJ 185. See also: Khaled El Emam et al, "Evaluating Predictors of Geographic Area Population Size Cutoffs to Manage Re-Identificaiton Risk" (2009) 16:2 JAMIA 256; Mei-Po Kwan, "Protection of Geoprivacy and Accuracy of Spatial Information: How Effective are Geographical Masks?" (2004) 39:2 Cartographica 15.

92 *Criminal Code*, R.S.C. 1985, c. C-46.

93 For example, s. 487.014 of the *Criminal Code* permits peace officers to ask persons to volunteer information that they are not otherwise prohibited by law from disclosing. Section 7(3)(c.1) of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [*PIPEDA*] similarly permits disclosure of information without consent by organizations "to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that" the information is required for the purposes of law enforcement, national security or the administration of a law of Canada or a province. Provisions with similar effect are found in British Columbia's *Personal Information Protection Act*, S.B.C. 2003, c. 63, S.A. 2003, c. P-6.5 [*PIPA* (B.C.)], s. 18(j), and Alberta's *Personal Information Protection Act*, S.A. 2003, c. P-6.5 [*PIPA* (Alberta)], s. 20(f).

94 See, for example, Oscar H. Gandy Jr., *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage*, (Ashgate, 2009); and Solove, *supra* note 86 at 47-48.

III. PRIVACY LAW AND LOCATION INFORMATION

Data protection legislation can place limits on the collection, use or disclosure of personal information and these limits may be instrumental in protecting the privacy of personal information. In this part of the paper, we begin with a discussion of data protection legislation in Canada. We consider the particular challenges posed by location-information for data protection regimes. We then address the broader privacy risks posed by location information, even where its collection, use or disclosure is carried out in a manner compliant with data protection norms.

(a) Data Protection and Location Information

In Canada, private sector data protection legislation sets a normative framework for the collection, use and disclosure of personal information. The federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to all inter-provincial collection, use and disclosure of personal information in the course of commercial activity, to the collection, use and disclosure of personal information by federal works and undertakings, and to intra-provincial activity where a province has not enacted substantially similar legislation.[95] Only Quebec, Alberta and British Columbia currently have general private sector data protection statutes that have been declared substantially similar.[96] In those three provinces, the applicable statute depends upon the nature of the activity at issue. In the context of location-based services, telecommunications operations will be subject to the federal legislation as they are federally-regulated undertakings. Some ISPs will fall under provincial law in Quebec, Alberta or British Columbia, while others may be governed by PIPEDA. Similarly, applications and location-based services that operate interprovincially will be subject to PIPEDA. A location-based service that is offered and that operates solely within one of the provinces with substantially similar legislation will likely be subject to the provincial legislation. The statutes are normatively quite similar, although there are significant differences at the level of enforcement and data security breach notification.

All of the private sector data protection statutes apply to the collection, use and disclosure of "personal information", and the definitions of personal information all centre on "information about an identifiable individual".[97] In the case of

---

95 *PIPEDA*, *supra* note 93, s. 4(1) and s. 26(2)(b).

96 In Quebec, *An Act respecting the protection of personal information in the private sector*, R.S.Q. c. P-39.1 was declared substantially similar by *Organizations in the Province of Quebec Exemption Order*, SOR/2003-374 (19 November 2003). Note that this statute predates *PIPEDA*. In Alberta, the *Personal Information Protection Act* (Alberta), *supra* note 93, was declared substantially similar by *Organizations in the Province of Alberta Exemption Order*, SOR/2004-219 (12 October, 2004). In British Colombia, the *Personal Information Protection Act*, SBC 2003, c. 63 was declared substantially similar by *Organizations in the Province of British Columbia Exemption Order*, SOR/2004-220 (12 October 2004).

97 *PIPEDA*, *supra* note 93, s. 2, definition of "personal information"; *PIPA* (B.C.), *supra* note 93, s. 1, definition of "personal information"; *PIPA* (Alberta), *supra* note 93, s. 1, definition of "personal information". The comparable Quebec legislation, *supra* note 96, uses slightly different wording, and provides, in s. 2, that "Personal information is

location information that tracks the movements of a mobile device, it might conceivably be argued that the information reveals the location of the device, but not necessarily the location of a specific individual, since the device might be shared or used by others. Nevertheless, as the EU Working Party notes, although mobile devices may be used by different people, such sharing is rare, and a "smart mobile device is very intimately linked to a specific individual."[98] Information on or about the devices should thus be considered "information about an identifiable individual."[99]

Specific pieces of information need not themselves disclose the identity of a particular individual to qualify as personal information, so long as it is reasonably possible to link that information to an identifiable individual.[100] Anonymized location information may still be personal information, if a company retains the means to link that information to specific individuals.[101] Further, if it is possible to identify an individual by examining patterns of movement and activity (for example, by drawing inferences about the location of the individual's home and workplace), then the information will constitute information about an identifiable individual.[102] Increasingly, data profiling activities result in the compilation of vast collections of

---

any information which relates to a natural person and allows that person to be identified".

98 Working Party 13/2011, *supra* note 26 at 7. See also Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (20 June 2007) 01248/07/EN WP 136, online: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf>.

99 Working Party 13/2011, *supra* note 26 at 10. Note that in PIPEDA Case Summary #351 — Use of personal information collected by Global Positioning System considered, online: <http://www.priv.gc.ca/cf-dc/2006/351_20061109_e.cfm>, the Assistant Privacy Commissioner found that tracking information from a GPS equipped vehicle was the personal information of the employee who drove that vehicle, because they could be specifically linked to it. The U.S. FTC also recommends applying its Privacy Framework to Information that can be linked to a specific device, and not just a specific individual: see Preliminary FTC Report, *supra* note 56.

100 See Teresa Scassa, "Geographic Information as Personal Information", (2010) 10:2 OUCLJ 185-214; *Gordon v. Canada (Minister of Health)*, 2008 FC 258, 324 F.T.R. 94, and *Ontario (Attorney General) v. Pascoe*, [2002] O.J. No. 4300, 166 O.A.C. 88, *(*sub nom. *Ontario (Attorney General) v. Ontario (Freedom of Information & Protection of Privacy Act Adjudicator))* 22 C.P.R. (4th) 447 (Ont. C.A.); affirming *Ontario (Attorney General) v. Ontario (Freedom of Information and Protection of Privacy Act Adjudicator)*, 16 C.P.R. (4th) 460 (Ont. Div. Ct.), *(*sub nom. *Ontario (Attorney General))* [2001] O.J. No. 4987, and Order P-230 (6 May 1991). The linking of de-identified information with other information so as to identify specific individuals can be surprisingly easy, given contemporary computing power and the vast array of public sources of data. See Preliminary FTC Report, *supra* note 56 at 106.

101 Working Party 13/2011, *supra* note 26 at 9. The FTC notes that the Unique Device Identifier in a mobile device can be combined with location information. When both sets of information are supplied to a third party mobile application provider, a specific user's location or activities can be revealed. See Preliminary FTC Report, *supra* note 56 at 36-37.

102 *Ibid* at 10.

atomized data particles into profiles that are effectively about identifiable individuals. The FTC observes that such practices blur the lines between what is personal information and what is non-personal information.[103]

PIPEDA applies specifically and only to personal information that is collected, used or disclosed in the course of commercial activity.[104] Mobile service providers are obviously engaged in commercial activity, whether it is telecommunication services or location-based services. Mobile device manufacturers and sellers are also engaged in commercial activity. Where apps are sold as through an interface like Apple's app store, the app developer is engaged in commercial activity. An app that is provided free of charge is in more of a grey area, although if the app collects personal information for the purposes of selling this data or using it in other commercial undertakings, this will no doubt be considered a collection in the course of commercial activity. Online businesses that offer "free" services, yet profit from the sale of advertising on their sites or that harvest and sell user data are engaged in commercial activity.[105]

The sharing of information between peers or "friends", however, does not implicate those peers in commercial activity (although the social networking service that also collects this information is engaged in commercial activity). Thus, PIPEDA would not apply to individuals who collect, use or disclose information about one or more of their social networking friends for their own purposes.[106] The B.C. and Alberta statutes also contain exceptions related to the collection, use or disclosure of personal information carried out for purely private purposes.[107]

Similar to its counterparts, PIPEDA is structured around 10 core normative principles. The first of these is accountability, and it requires that organizations that engage in the collection, use or disclosure of personal information clearly designate a person responsible for data protection compliance, and develop appropriate policies and practices.[108] They must also train staff and develop procedures with a

---

103 Preliminary FTC Report, *supra* note 56 at 36.

104 *PIPEDA*, *supra* note 93 s. 2, applies only to information that is collected, used, or disclosed in the course of "commercial activity," which is defined in the Act as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists".

105 For example, the Office of the Privacy Commissioner of Canada accepted that Facebook was engaged in commercial activity, even though its services are free to consumers, when it proceeded with its inquiry into the activities of that company; see PIPEDA Case Summary #2009-008, Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the *Personal Information Protection and Electronic Documents Act*, online: <http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf> [Facebook Complaint].

106 For example, *PIPEDA*, *supra* note 93, s. 4(2)(b) provides that its provisions do not apply to "any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose". Similar exceptions can be found in *PIPA* (B.C.), s. 3(2)(a) and *PIPA* (Alberta) s. 4(3)(a).

107 *PIPA (Alberta)*, *supra* note 93, s. 3(a); *PIPA* (B.C.), *supra* note 93, s. 3(a).

108 *PIPEDA*, *supra* note 93, Schedule I, principle 4.1.

view to protecting data privacy. The second principle requires organizations to identify the purposes for which they are collecting personal information at or before the point in time when that information is collected.[109] This is a notice requirement, and service providers and developers must find ways to give adequate notice to consumers not just of the fact that personal information is being collected, but also of the purposes for the collection. Adequate notice has been a recurring issue with location-based services.

Like other online services, location-based services may use default settings as a means of simplifying the process of initiating the service. Nevertheless, default settings may not give users the appropriate degree of notice. In her discussion of default privacy settings in a complaint brought against Facebook, the Assistant Privacy Commissioner of Canada expressed the view that it might be appropriate to use default settings that would facilitate the registration process for the site, "provided that the default settings are reasonable and the users properly informed of them."[110] The Assistant Commissioner found that some of the Facebook default settings were not reasonable, and she further found that Facebook had not done all that it should to inform users about the defaults. She wrote: "On the registration pages, there is no direct link to the privacy settings and no upfront message about these settings and the fact that they have been preselected by Facebook and can be changed."[111]

Notice has also been an issue in the location-based services field, where there have been a number of instances of apps that collect personal information with no notice to consumers. Some of these have not even been apps where the need to collect personal information about location is evident.[112] The problem is compounded by the trans-border nature of this industry. Apps developed in a jurisdiction with few data protection restrictions, such as the U.S., may be available to Canadian users through online downloads, even if they are not compliant with Canadian data protection norms.

Consent is a cornerstone principle in data protection legislation; essentially the legitimation of the collection, use and disclosure of personal information is premised upon the data subject's consent to these activities. In reality, consent requirements have proven problematic. In some cases, "opt-out" forms of consent have been used, where consumers must check a box or otherwise indicate their withdrawal of consent to information collection and/or sharing.[113] Where the opt-out option is buried in a privacy policy, or is part of default settings, this may diminish

---

109 *PIPEDA*, *supra* note 93 Schedule I, principle 4.2.

110 Facebook Complaint, *supra* note 105 at para. 89.

111 *Ibid* at para. 96.

112 Thurm & Kane, *supra* note 28.

113 *PIPEDA*, *supra* note 93 Schedule 1, clause 4.3.7 permits opt out consent in specific circumstances. In PIPEDA Case Summary #2002-42 (Update), online: <http://www.priv.gc.ca/cf-dc/2002/cf-dc_020320_e.cfm>, the Privacy Commissioner linked the sensitivity of the information at issue to the question of whether "opt-out" was an appropriate means by which to seek consent. See discussion of this case by Lisa M. Austin, "Is Consent the Foundation of Fair Information Practices? Canada's Experience under PIPEDA", (2006) 56 UTLJ 181 at 207-208.

the credibility of any consent.[114] Some case law suggests that opt-out consent is appropriate only with information of a very low level of sensitivity.[115] This would not include location information, which should generally be considered highly sensitive,[116] particularly where it reveals patterns of activity.

Consent can also be problematic where it is difficult for an ordinary consumer to grasp the full implications of their consent to collection, use or disclosure of personal information. In the U.S., the FTC notes that it is a significant concern that consumers are unable to make informed choices due to a lack of understanding of data collection and use practices.[117] It is interesting to note that Bill C-29[118] would have added a new section 6.1 to PIPEDA, which would have read: "For the purposes of clauses 4.3 to 4.3.8 of Schedule 1, the consent of an individual is *only valid if it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure of personal information to which they are consenting*."[119] This would have marked a significant change, placing a much greater onus on organizations to clarify the consequences to the individual of the collection, use or disclosure of their personal information. The amended consent provision might also have enhanced obligations to ensure that the terms of consent are drafted in an accessible manner that is appropriate to the clientele for the service.[120] It remains to be seen whether a comparable provision will be part of the next PIPEDA reform bill to be introduced in Parliament.

Consent must be specific to the identified purposes for collection of information. In other words, the consent must be for those purposes, and not for some broader, more general form of activity. Where new purposes are introduced, new notice must be given and a fresh consent obtained.[121] In its *Opinion on geolocation services*, the EU Working Party also recommended that service providers should seek renewal of consents periodically, where services are used on an ongoing basis.[122]

While consent must in most cases be explicitly given, implied consent may be

---

114 Preliminary FTC Report, *supra* note 56 at 60.

115 *PIPEDA*, *supra* note 93, Schedule 1, clause 4.3.6. See: PIPEDA Case Summary #2003-203 (5 August 2003), online: <http://www.priv.gc.ca/cf-dc/2003/cf-dc_030805_01_e.cfm>; Case Summary #2003-192 (23 July 2003), online; <http://www.priv.gc.ca/cf-dc/2003/cf-dc_030723_01_e.cfm>.

116 See, e.g., Working Party 13/2011, *supra* note 26 at 14. The Working Party also notes that opt out consent is not appropriate.

117 Preliminary FTC Report, *supra* note 56 at 25.

118 Bill C-29, *An Act to amend the Personal Information Protection and Electronic Documents Act*, 3d Sess, 40th Parl, 2010. This *PIPEDA* reform Bill died on the order paper prior to the May 2, 2011 federal election. At the time of writing it is unclear if it will be reintroduced, and if so, whether it will be identical to the previous bill.

119 *Ibid* [emphasis added].

120 The Working Party 13/2011, *supra* note 26 at 18, notes that service providers should not presume a technically sophisticated clientele.

121 *PIPEDA*, *supra* note 93, Schedule 1, clause 4.3.1. See also Working Party 13/2011, *supra* note 26 at 15.

122 *Ibid* at 15-16.

appropriate in some circumstances. PIPEDA provides that implied consent will typically only be appropriate with information that is considered to be of a less sensitive character,[123] which would not include location information. However, implied consent may also be considered acceptable where "at the time the consent is deemed to be given, the purpose would be considered to be obvious to a reasonable person."[124] The location of an individual might be considered information that is obviously required for the delivery of mobile services that the user has requested. This might include, for example, where the user requests a list of restaurants close to their location, or where they have subscribed to the delivery of mobile telecommunications services generally. However, it will be less obvious to a reasonable person that their location information must be collected, used or disclosed to deliver to services that they did not specifically ask to receive, such as unsolicited mobile marketing information.

Certain services or applications may have default privacy settings which, unless altered by the user, might indicate that they have consented to the collection, use or disclosure of personal information. In the *Facebook Complaint*, the Assistant Privacy Commissioner of Canada was prepared to accept the expedient use of some default settings, presumably as a proxy for consent. Nevertheless, she tied the legitimacy of the choice of defaults to "whether the default privacy settings meet the reasonable expectations of Facebook users."[125] By contrast, the EU Working Party on geolocation services expressed the view that default settings should not be interpreted as consent. They wrote: "If the default settings of an operating system would allow for the transmission of location data, a lack of intervention by its users should not be mistaken for freely given consent."[126]

Consent issues may also arise where End User Licence Agreements (EULAs) or other standard form contracts contain clauses which provide that consumers who "agree" to the terms of the EULA consent to the collection, use or disclosure of their personal information. This may be particularly problematic in the context of privacy policies displayed on mobile devices, where it may be necessary to scroll through a large number of screens in order to view the entire policy.[127] The FTC specifically recommends that "[c]ompanies that provide services on mobile and other "small screen" hand-held devices should determine how best to ensure that consumers can access and review pertinent information about data practices."[128]

---

123 *PIPEDA*, *supra* note 93, Schedule 1, clause 4.3.4. See also: *Randall v. Nubody's Fitness Centres*, 2010 FC 681.

124 *PIPA* (B.C.), *supra* note 93, s. 8(1)(a). Note that this provision at s. 8(1)(b) also requires that "the individual voluntarily provides the personal information to the organization for that purpose". A comparable provision is found in s. 8(2) of *PIPA* (Alberta), *supra* note 93. See also *PIPEDA*, *supra* note 93, Schedule 1, clause 4.3.5. Principle 4.3.5 refers to the reasonable expectations of the individual, and gives the example of the need to use subscriber name and address in order to deliver a magazine subscription.

125 Facebook Complaint, *supra* note 105 at para. 89.

126 Working Party 13/2011, *supra* note 26 at 14.

127 Preliminary FTC Report, *supra* note 56 at 70-71.

128 *Ibid* at 71.

The EU Working Party provides that "consent cannot be obtained freely through mandatory acceptance of general terms and conditions, nor through opt-out possibilities."[129] However, Canadian courts have found standardized form contracts sufficient to reflect a consumer's consent to certain disclosures of personal information.[130] This is in spite of the fact that standard form privacy policies have become notoriously lengthy and difficult to read[131] and offer consumers few, if any real choices. Consent is thus compromised both because it is not sufficiently informed, and because it may not be truly voluntary.[132] The FTC has observed that: "Too often, privacy policies appear designed more to limit companies' liability than to inform consumers about how their information will be used."[133]

Once consent is given, it may be appropriate to seek renewal of that consent, especially where information is automatically provided by the consumer on an ongoing basis. This might be the case, for example, where a mobile device regularly and repeatedly communicates its location over the life of the device.[134] Where privacy policy terms change, during the course of the relationship between the consumer and the company, fresh consent to the new terms should be obtained, and this should be done in a transparent manner. For example, the FTC suggests that "before making material changes to their data policies, companies should make prominent disclosures that clearly describe such changes, and should obtain consumers' affirmative consent."[135]

PIPEDA and its provincial counterparts all foresee certain circumstances in which collection, use or disclosure of personal information can be made without an individual's knowledge or consent.[136] These may include circumstances in which

---

129 Working Party 13/2011, *supra* note 26 at 14.

130 *Gomboc*, *supra* note 3. See also *R v. Cuttell*, 2009 ONCJ 471, [2009] O.J. No. 4053 [*Cuttell*], *R v. Vasic* (2009), 185 C.R.R. (2d) 286, [2009] O.J. No. 685 (Ont. S.C.J.) [*Vasic*]; *R v. Ward*, 2008 ONCJ 355 [*Ward*] and *R v. Wilson* (February 10, 2009), Doc. St. Thomas 4191/08 (Ont. S.C.J.) [*Wilson*]. While it is true that these cases are in the criminal context, and deal with whether there is a reasonable expectation of privacy for constitutional privacy purposes, the courts nevertheless did find that the existence and terms of the standard form contracts (which indicated that personal information could be provided to law enforcement officials without notice or consent) were sufficient to negate the customer's reasonable expectation of privacy in their personal information.

131 See, e.g., Felicia Williams, *Internet Privacy Policies: A Composite Index for Measuring Compliance to the Fair Information Principles*, (2006) at 17-18, online: <http://www.ftc.gov/os/comments/behavioraladvertising/071010feliciawilliams.pdf>.

132 Note that Canadian data protection statutes require that consent to the collection, use or disclosure of personal information not be made a condition of receiving goods or services, beyond what is required in order to provide the goods or services. See, e.g.: *PIPA* (B.C.), *supra* note 93, s. 7(2); *PIPA* (Alberta), *supra* note 93, s. 7(2); *PIPEDA*, *supra* note 93, Schedule 1, clause 4.3.3.

133 Preliminary FTC Report, *supra* note 56 at 19.

134 Working Party 13/2011, *supra* note 26 at 15-16.

135 Preliminary FTC Report, *supra* note 56 at 69.

136 Section 7(1) of *PIPEDA*, *supra* note 93, details the limited occasions in which it would be "inappropriate" to require the individual's knowledge and consent: a) the collection is clearly in the individual's interests and consent cannot be obtained in timely way; b)

an individual's life is in jeopardy. For example, a service provider might disclose information about the location information on a user's mobile device if it is suspected that the user is in a situation of peril and requires assistance.[137] Many of the exceptions to consent relate to law enforcement, court orders, debt collection or the administration of laws.[138] These provisions raise the possibility that a court may order, in the context of civil litigation, the disclosure of an individual's location information considered relevant to some aspect of the litigation.[139] There are also exceptions to consent requirements for journalistic activities,[140] and publicly available information.[141]

A fourth principle relates to limitations on the collection of personal information. Organizations are required to limit their collection of information to what is reasonable for the purposes that they have specified. This principle introduces a reasonableness concept which is complementary to that in s. 3 of PIPEDA. Section 3 limits the collection, use and disclosure of personal information by organizations to "purposes that a reasonable person would consider appropriate in the circumstances."[142] Thus the collection, use or disclosure of personal information must be for reasonable purposes, and must be limited to what is reasonable to meet those purposes.[143] Canadian courts have emphasized the compromise nature of data protection legislation. In a recent Federal Court decision, Mainville J. stated: "PIPEDA is a compromise between competing interests, and its provisions must be inter-

---

it is reasonable to expect that the collection with the individual's knowledge or consent would compromise the information's accuracy or availability and the collection is reasonable for investigating legal breaches; c) the collection is only for journalistic, artistic or literary purposes; or d) the information is publicly available. Information that is publicly available is specified in the regulations: *Specifying Publicly Available Information, Regulations*, SOR/2001-7.

137 *PIPEDA*, *supra* note 93, ss. 7(1)(a), 7(2)(b), 7(3)(e); *PIPA* (Alberta), *supra* note 93, ss. 14(a), 17(a), 20(a), (g); *PIPA* (B.C.), *supra* note 93, ss. 12(a), 15(a), 18(a), (k).

138 *PIPEDA*, *supra* note 93, ss. 7(3)(c.1), 7(3)(c), 7(3)(b); *PIPA* (Alberta), *supra* note 93, ss. 4(3)(c); 14(b), (c.2), (i); s. 17(b), (d), (j); s. 20(b), (f), (i); *PIPA* (B.C.), *supra* note 93, ss. 3(2)(b); 12(j), (e); s. 15(j), (e); s. 18(e), (g), (i), (j).

139 See, e.g.: *Kocsis v. Kocsis* (July 14, 2005), Doc. Barrie 209-05 (Ont. S.C.J.).

140 *PIPEDA*, *supra* note 93, s. 4(2)(c), s. 7(1)(c); *PIPA* (Alberta), *supra* note 93, s. 4(3)(c); *PIPA* (B.C.), *supra* note 93, s. 3(2)(b). See Teresa Scassa, "Journalistic Purposes and Private Sector Data Protection Legislation: Blogs, Tweets, and Information Maps" (2010) 35 Queen's LJ 733.

141 *PIPEDA*, *supra* note 93, ss. 7(1)(d), 7(2)(c.1), 7(3)(h.1); *PIPA* (Alberta), *supra* note 93, ss. 14(e), 17(e), 20(j); *PIPA* (B.C.), *supra* note 93, ss. 12(e), 15(e), 18(e). Each statute specifically defines information that is available to the public. It typically includes public directory and registry information.

142 *PIPEDA*, *supra* note 93, s. 3. *PIPA* (Alberta), *supra* note 93, s. 2(b), defines reasonableness as "what a reasonable person would consider appropriate in the circumstances".

143 The provincial data protection statues combine these requirements in an explicit norm. See, e.g.: *PIPA* (Alberta), *supra* note 93, s. 11. The Preliminary FTC Report, *supra* note 56 at 45-46, also talks about limiting data collection to only that information necessary to fulfill a specific business need.

preted and applied with flexibility, common sense and pragmatism."[144] In a decision under Alberta's PIPA, the majority of the Alberta Court of Appeal indicated that the "reasonableness" standard required a recognition of the twin underlying considerations of the Act. According to the Court, these are "the rights of the individual to a reasonable level of privacy, and the needs of organizations to make reasonable use of information on the conduct of their activities."[145] In expressing this view, the majority also indicated that this balance of rights did not require companies to adopt a "minimalist" approach to data collection.[146]

A fifth principle similarly places limits on the use, disclosure and retention of personal information, requiring that any such use or disclosure be for the specified purposes for which consent was given.[147] Under PIPEDA personal information shall be retained only as long as necessary for the fulfilment of the specified purposes. As data collection expands, and as data security breaches become increasingly common and potentially devastating, much greater attention has been given to the issue of data retention.[148] In the context of location-based information, while it may be important for mobile device providers to collect this information to allow

144 *State Farm Mutual Automobile Insurance Co. v. Canada (Privacy Commissioner)*, 2010 FC 736 at para. 101.

145 *Leon's Furniture Ltd. v. Alberta (Information & Privacy Commissioner)*, 2011 ABCA 94 [*Leon's*] at para. 38. See also a comparable view on the twin purposes of PIPEDA in *Englander v. Telus Communications Inc.*, 2004 FCA 387, [2005] 2 F.C.R. 572 at para. 46.

146 *Leon's*, *supra* note 145 at para. 38. Leave to appeal to the Supreme Court of Canada is being sought. In general, data protection commissioners have taken a firmer line in limiting the collection of data to reasonable purposes and to the extent reasonable for those purposes. See, for example, See, for example: *Cruz Ventures Ltd (cob Wild Coyote Club)(Re)*, [2009] BCIPCD No 16, online: <http://www.oipc.bc.ca/PIPAOrders/2009/OrderP09-01.pdf>; PIPEDA Case Summary #396, [2008] SCCPVPC No 9, online: <http://www.priv.gc.ca/cf-dc/2008/396_20080227_e.cfm>; *Penny Lane Entertainment Group v. Alberta (Information & Privacy Commissioner)*, 2009 ABQB 140, [2009] A.W.L.D. 2633 (Alta. Q.B.).

147 Of course, statutory exceptions also apply to the general requirement of consent to use or disclosure. Such exceptions permit information to be used or disclosed without consent for other purposes (such as law enforcement, debt collection, or the administration of laws).See, for example, *PIPEDA*, *supra* note 93, s. 7(2) and (3).

148 In her report of an investigation into the security, collection and retention of personal information: *TJX Companies Inc/Winners Merchant International LP*, (25 September 2005) online: <http://www.priv.gc.ca/cf-dc/2007/tjx_rep_070925_e.cfm>, the Assistant Privacy Commissioner of Canada was critical of the companies' collection of excessive amounts of personal information and of the retention of this information for an unnecessarily long period of time. See also: Jeremy Warner, "The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps", (2005) 2 UOLTJ 75, online: <http://www.uoltj.ca/articles/vol2.1/2005.2.1.uoltj.Warner.75-104.pdf>; Jean-François Blanchette & Deborah G. Johnson, "Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness", (2002) 18 The Information Society 33. Data retention is also addressed by the Preliminary FTC Report, *supra* note 56 at 47, where it writes: "businesses should promptly and securely dispose of data, including paper and electronic records, for which they no longer have a specific business need".

the mobile device to function quickly and efficiently, it is not clear that it is necessary to retain this information for any significant period of time.[149] For example, one of the "fixes" proposed by Apple, in the wake of the uproar over the collection of location information via the iPhone 4 was to ensure that such information is only stored for short periods of time.[150] Because location information may have significant commercial value to data profilers and mobile marketers, the interest in retaining this information for longer periods of time with a view to selling it for other purposes may be high. However, such practices put consumers at risk, and might well contravene data protection laws. The FTC specifically notes that location-based data should not be retained for longer than is necessary because of the heightened risk to privacy posed by the sensitive nature of this information.[151]

Organizations are required to be transparent about their policies and practices with respect to personal information. Although transparency requires the communication of information about an organization's policies, it may also require that such information be communicated in an accessible manner. In its recently released Privacy Framework, the U.S. Federal Trade Commission linked the value of transparency to clear, shorter and more standardized privacy policies.[152] The FTC also suggested that mechanisms that permit consumers to compare data practices of different companies would enhance both transparency and competition with respect to privacy protective measures.[153]

Data protection norms also require organizations to ensure that personal information that they collect is "as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used."[154] A related principle is that of access; individuals have a right to access their personal information in the hands of private sector organizations, and to request that any inaccurate or incomplete information be amended. The EU Working Party on geolocation services expressed the view that when providing access to individuals' geolocation information, companies should ensure it is in "human readable format", with specific geographic locations rather than making reference to the numeric identifiers or coordinates.[155] The access principle also requires organizations to indicate, to the extent possible, those other organizations to which it has disclosed the individual's personal information.

Organizations must also ensure that they have sufficient safeguards in place to protect the personal information of individuals. The more sensitive information is, the greater the obligation to protect that information.[156] Location information, particularly where it shows a pattern of activity over time, is likely to be considered

149 Working Party 13/2011, *supra* note 26 at 19.

150 Joelle Tessler, "Senate panel grills Apple, Google on location data", *Bloomberg Businessweek* (10 May 2011) online: <http://www.businessweek.com/ap/financialnews/D9N4ONJ01.htm>.

151 Preliminary FTC Report, *supra* note 56 at 47.

152 *Ibid* at 41.

153 *Ibid* at 69.

154 *PIPEDA*, *supra* note 93, Schedule 1, clause 4.6.

155 Working Party 13/2011, *supra* note 26 at 18.

156 See for example, Preliminary FTC Report, *supra* note 56 at 45; and *PIPEDA*, *supra* note 93 Schedule 1, clause 4.7.2.

highly sensitive, and companies that collect this information will have strict obligations to ensure its security. Obligations in this regard relate to security measures to protect the information in the hands of the organization (such as encryption, firewalls, or other security measures), as well as obligations to ensure its safe destruction once the need for the information has come to an end. There have been enough high-profile data security breaches in recent years to provide heightened scrutiny of these issues. The Alberta private sector data protection legislation was amended in 2009 to include data security breach notification provisions,[157] and proposed amendments to PIPEDA in the late Bill C-29 would also have imposed a limited data security breach notification obligation on organizations governed by that law.[158] On May 4, 2011, the Office of the Privacy Commissioner of Canada issued a press release calling on the government to reintroduce a much stronger data security breach notification obligation, and to give the Commissioner the power to impose significant fines on companies in the case of significant breaches.[159]

Enforcement of obligations under private sector data protection legislation has become an increasingly important issue in recent years, particularly under PIPEDA. In the first place, there may be significant jurisdictional hurdles to overcome in dealing with complaints. In many cases where location-based services are concerned, the companies engaged in the collection, use or disclosure of personal information may be located in a different country — often the United States. Questions have been raised about the ability of the federal Privacy Commissioner to initiate investigations against such companies. In *Lawson v Accusearch Inc*,[160] the Federal Court ruled that, where there was a sufficient connection to Canada, the Privacy Commissioner had the jurisdiction to investigate. In that case, the Complainant was Canadian and her personal information had been collected, presumably from Canadian sources, and disclosed in Canada by a company based in the United States. The court concluded that "PIPEDA gives the Privacy Commissioner jurisdiction to investigate complaints relating to the transborder flow of personal information."[161] That being said, the court acknowledged that there might be significant barriers to the investigation, particularly where the foreign-based company declined to co-operate. Some of these difficulties might be overcome through the use of Mutual Legal Assistance Treaties with other countries, or other memoranda of understanding.[162]

---

157 The amendments were in *Bill 54: Personal Information Protection Amendment Act, 2009* which received third reading on November 18, 2009 and which came into force on May 1, 2010.

158 Bill C-29, *supra* note 118, ss. 10.1–10.3.

159 Office of the Privacy Commissioner of Canada, News Release, "Fines Needed to Help Stem Growing Data Breaches, Privacy Commissioner Says" (4 May 2011), online: <http://www.priv.gc.ca/media/nr-c/2011/nr-c_110504_e.cfm>.

160 2007 FC 125, [2007] 4 FCR 314 [*Lawson*].

161 *Ibid* at para. 51.

162 Steve Coughlan et al, "Global Reach, Local Grasp: Constructing Extraterritorial Jurisdiction in the Age of Globalization" (2007) 6 CJLT 29 at 46. Following the decision in *Lawson*, *supra* note 160, the OPC proceeded with its investigation of Accusearch. It

The investigation into the complaint against Facebook offers an interesting example of what can be achieved even absent the powers to physically investigate a company based in another country or to compel the production of documents. In that case, California-based Facebook chose to voluntarily cooperate with the Privacy Commissioner's investigation. Perhaps more importantly, the company took steps to implement the recommendations which flowed from the investigation. Absent this level of cooperation, it would have been necessary for either the Commissioner or the Complainant to take the matter to federal court for a court order. Whether any such order, if obtained, would have been enforced against the company by a U.S. court is an open question.

Not all companies based outside of Canada are likely to cooperate to the same extent as Facebook should they face an investigation by the OPC. Indeed, the Facebook complaint was strategically well chosen because the company was large, high profile, and had a high volume of Canadian-based users. Smaller companies will be much less concerned about any possible media backlash against them, and may not have a significant enough base of Canadian users to make cooperation worth their while.

Trans-border issues are not the only challenge for the enforcement of data protection laws in Canada. Although the provincial private sector data protection statutes provide the relevant provincial commissioners with binding order-making powers, the Federal Privacy Commissioner has no such authority under PIPEDA. Instead, the OPC is limited to playing the role of an ombudsperson, and merely issues findings and recommendations.[163] Where a company ignores the recommendations, either the complainant or the Privacy Commissioner may take the matter to Federal Court.[164] A complainant may also apply to Federal Court for a remedy that may include monetary compensation.[165] This two-stage process at the federal level is time-consuming, and also places significant costs on the individual complainant. The cumulative effect is that the enforcement mechanisms for PIPEDA are weak.

The shaming of companies who have engaged in poor information handling

---

was evident from the report of findings in this case that without the assistance of the FTC, which was engaged in its own concurrent investigation of Accusearch, little would actually have been learned about the company's activities. See: *Commissioner's Findings — PIPEDA Case Summary #2009-009: — Complaint under PIPEDA against Accusearch Inc., doing business as Abika.com — July 31, 2009*, online: <http://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.cfm>.

163 For a critique of the ombuds model for data protection in Canada see: Christopher Berzins, "Three Years Under the PIPEDA: A Disappointing Beginning" (2004) 3 CJLT 113; John Lawford, "Consumer Privacy Under PIPEDA: How Are We Doing?" (Ottawa: Public Interest Advocacy Centre, November, 2004) at 13, retrieved from: http://www.piac.ca/PIPEDAReviewFinal.pdf; Colin J. Bennett, "The Privacy Commissioner of Canada: Multiple Roles, Diverse Expectations and Structural Dilemmas" (2003) 46:2 *Canadian Public Administration* 218. See also: Jennifer Stoddart, "Cherry Picking among Apples and Oranges: Refocusing Current Debate about the Merits of the Ombuds-Model Under PIPEDA" (21 October 2005) online: <http://www.priv.gc.ca/information/pub/omb_051021_e.cfm>.

164 *PIPEDA*, *supra* note 93, ss. 14, 15.

165 *Ibid*, ss. 14, 16.

practices may be a useful tool in encouraging compliance. While the provincial privacy commissioners all disclose the names of respondent companies in complaints, this is not done at the federal level, unless there are exceptional circumstances. This approach has been criticized as further undermining already weak enforcement mechanisms.[166] While it is possible that PIPEDA reform may eventually address some of these lacunae, it should be noted that apart from a new data security breach notification requirement, significant enforcement reforms were lacking in Bill C-29.

(b) The Intersection of Data Protection Laws with Constitutional Privacy Norms

Location-based information is of great interest to law enforcement and national security officials in a wide range of contexts. Information that reveals an individual's movements over periods of time has frequently been important in criminal and other investigations. Where such information is directly gathered by law enforcement officials, warrants are typically required for anything other than visual surveillance. In such a context, location information collected by private sector companies may be particularly attractive to law enforcement officials. Not only can such information be detailed and fine-grained, it may also be historical (relating to periods prior to the commission of a crime or prior to a warrant being sought).

Location-based information in the hands of third party organizations may also be easier to access, as data protection laws may create possibilities for law enforcement officials to seek this information from third parties without need for a warrant. For example, section 7(3)(c.1) of PIPEDA, as well as comparable provisions in the private sector data protection statutes of British Columbia and Alberta[167] permit organizations to disclose customer information to law enforcement officials for investigation purposes without the knowledge or consent of the data subject. The laws are permissive only — organizations are not required to disclose on request, and may insist upon a court order before disclosing. In a series of cases under PIPEDA, courts have grappled with the relationship of section 7(3)(c.1) to the right in section 8 of the *Canadian Charter of Rights and Freedoms* to be free from unreasonable search or seizure.[168] At the heart of these cases is whether the permissive provisions obviate the need for a court order where organizations are willing to provide the information on request. The jurisprudence is not settled, but it would seem to turn on whether the accused had a reasonable expectation of privacy in the information.

The concept of the reasonable expectation of privacy is relied upon in the constitutional privacy jurisprudence of both Canada and the United States.[169] Essentially, the state cannot be found to violate an individual's privacy if that citizen did

166 Berzins, *supra* note 163; Bennett, *supra* note 163.

167 *PIPA* (B.C.), *supra* note 93, s. 18(1)(j); *PIPA* (Alberta), *supra* note 93 s. 20(f).

168 *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [*Charter*] s. 8.

169 See, for example: *US v Katz*, 389 US 347 (1967). In Canada, the reasonable expectation of privacy is central to an analysis of the s. 8 right to be free from unreasonable search and seizure. See, for example: *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145;

not have a *reasonable* expectation of privacy in the circumstances. The reasonable expectation of privacy has come under increasing pressure in our technological society. It has been criticized by some for setting a standard which allows changing technology and changing law enforcement or commercial practices to degrade privacy protection by simply undermining our expectations.[170] The Supreme Court of Canada has responded to this concern by stating that the reasonable expectation of privacy should not depend upon the reasonableness of one's expectations in a context in which privacy is increasingly eroded by technologies of surveillance and data collection. Instead, a court's analysis should consider the balance between one's privacy interests and other compelling public interests.[171]

Where the subject matter of the search is information, courts apply an "informational privacy" analysis.[172] Such analysis focuses upon "the thorny question of how much *information* about ourselves and activities we are entitled to shield from the curious eyes of the state."[173] Canadian courts have used a "spectrum" approach as part of the informational privacy analysis, placing the "biographical core of personal information,"[174] at the high end of the scale of protection. Core biographical information was described in *R v. Plant*[175] as information: "which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual."[176] Location information would clearly be core biographical information.[177]

Plant, *supra* note 3; *R v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432 [*Tessling*]; *R v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579 [*Patrick*]; and *Gomboc*, *supra* note 3.

170 See, for example: James A.Q. Stringham, "Reasonable Expectations Reconsidered: A Return to the Search for a Normative Core for Section 8?" (2005), 23 CR (6th) 245 at 251. Solove also discusses the social impact of the normalization of surveillance: see Solove, *supra* note 86 at 35. Nissenbaum is also critical of the effects of practice and convention on expectations of privacy. See Helen Nissenbaum, "Privacy as Contextual Integrity", (2004) 79 Wash. L. Rev. 119 at 144.

171 *Patrick*, *supra* note 169 at para. 14 and *Tessling*, *supra* note 169 at para. 42.

172 The Supreme Court of Canada has described informational privacy as those privacy interests that lie "[b]eyond our bodies and the places where we live and work"; see *ibid* at para. 23.

173 *Ibid* [emphasis in the original].

174 See *Plant*, *supra* note 3 at 293.

175 *Ibid.*

176 *Ibid* at 293.

177 See, e.g., Working Party 13/2011, *supra* note 26 at 14. Some case law has made distinctions, in terms of the expectation of privacy, based on the precision or quality of the information. This was certainly the case in both *Tessling*, *supra* note 169 at 29, and *Gomboc*, *supra* note 169 at para. 40. In *Tessling*, the heat signature information was considered to be usable only to draw inferences about possible activities within the home. Similarly, four of the judges in *Gomboc* found that the data about the patterns of electrical consumption was useful only to draw inferences. In the case of location information, the particular positioning technology in use may be considered relevant. For example, in one U.S. case, location information consisting of the individual's position based on the nearest cell phone tower was considered to be sufficiently imprecise as

A key factor in the contextual analysis of the reasonable expectation of privacy in information which is set out in *R v. Tessling*,[178] and which was considered by the Supreme Court of Canada most recently in *R v. Gomboc*,[179] is whether the information gathered by the police was in the hands of a third party, and if so, what were the expectations of confidentiality related to that information. The U.S. Supreme Court has ruled that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties,"[180] and the Supreme Court of Canada in *Plant*[181] similarly found a very much diminished expectation of privacy in information in the hands of third party service providers.

It is at this point that the intersection of data protection legislation and the reasonable expectation of privacy is most explicit. As noted above, data protection legislation expressly contemplates that third parties will collect data from data subjects, and the terms and conditions upon which such collection will take place. Typically a company will have a privacy policy that explains how customer information will be handled. In Section 8 *Charter* cases involving police access to information in the hands of third parties, privacy policies have been treated by courts as setting the boundaries for the reasonable privacy expectations of consum-

---

not to raise constitutional privacy concerns. *In Matter of Application of US for an Order*, 411 F Supp 2d 678, 682 (WD La 2006). See also *In re Application of the United States For An Order For Disclosure of Telecommunication Records And Authorizing the Use of A Pen Register and Trap and Trace*, 405 F.Supp.2d 435, 449-450 (S.D.N.Y. 2005). An opposite conclusion was reached in *In Re Application Of The United States For An Order For Prospective Cell Site Location Information On A Certain Cellular Telephone*, 2006 US Dist LEXIS 11747 (S.D.N.Y. 2006), online: <http://www.eff.org/files/filenode/celltracking/SDNY_cell_site_II_denial.pdf>. However, these cases can be contrasted with the Ontario Superior Court's decision in *R. v. Mahmood* (2008), 236 C.C.C. (3d) 3 (Ont. S.C.J.); additional reasons [2009] O.J. No. 3192, 194 C.R.R. (2d) 180 (Ont. S.C.J.) where the data collected from cell phone towers about thousands of users within the area, was relatively imprecise beyond indicating that those individuals were in the particular area within a key window of time. The court nevertheless found that police trawling through this data was privacy invasive. Of course, as noted earlier, the technological trend is towards increasingly accurate location information. The presence of GPS chips in an increasing number of mobile devices, for example, means that the precision of location data obtained from cell phone use will inevitably be enhanced. Courts must be wary of location information precedents based on older forms of technology offering inferior data quality.

178 *Supra* note 169.

179 *Supra* note 3.

180 *Smith*, *supra* note 3. More recent U.S. case law suggests that when it comes to records of movements in the hands of service providers, the situation is unsettled. In *In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, *supra* note 3, the motions judge found that citizens had a reasonable expectation of privacy in their location and movements as recorded in cell phone usage information. This decision was reversed by the court of appeals, which found that it cannot be assumed that cell phone records will automatically amount to tracking data that extends into the private realm of the home. (620 F 3d 304 (3d Cir Pa 2010)).

181 *Plant*, *supra* note 3.

ers. For example, where a privacy policy explicitly states that the information collected by the company may be shared with law enforcement officials without the knowledge or consent of the data subject, courts have been willing to find that the data subject has no reasonable expectation of privacy in that information when it is disclosed in accordance with the terms of the policy.[182] This view is based on the idea that the consumer has consented to the terms of the privacy policy, and thus cannot be surprised if such information sharing actually takes place. Of course, this is all premised on notions of consent. As noted above, serious issues arise regarding consent to terms found in standard form contracts, default settings and the like. Unfortunately, if such consents are considered valid in the data protection realm, there may be relatively little protection for customer information. In *Gomboc*, the Supreme Court of Canada was split as to whether an obscure regulation governing electrical utilities that required customers to opt out of voluntary data sharing with authorities, could negate any expectation of privacy in customer data. A majority of judges was of the view that it was either determinative, or was a relevant factor to consider. Privacy policies, so seldom read by consumers,[183] may thus play a key role in determining their reasonable expectation of privacy vis à vis law enforcement officials in their location information.

When dealing with information as highly personal as location information, the presence of a clause in a service provider contract that states that information may be shared with police without the customers notice or consent should not be treated as sufficient to automatically eliminate a reasonable expectation of privacy. Where such clauses are buried in privacy policies attached to standard form contracts, they may simply have never been read by the consumer. Further, in contracts where the customer has limited or no bargaining power, or where there are few other service alternatives, such clauses should not be used to obviate a reasonable expectation of privacy in information as sensitive as one's movements and activities.

The vastly increased amounts of data captured by service providers in the information age may be injecting more nuances into these discussions. As McLaughlin notes, the rise of mobile marketing and the decline of data storage costs may both contribute to the retention of a high volume of relatively fine grain location information.[184] An arguable case can be made that this should heighten judicial concerns about privacy with respect to this information.

IV. TECHNOLOGICAL PRIVACY PROTECTION

Numerous technological measures have been advanced to solve privacy issues associated with location-based technologies. Some of these mechanisms offer complete protection of personal data, while others offer merely partial protection, but a

182 See, e.g., *Ward*, *supra* note 130; *Cuttell*, *supra* note 130; *Vasic*, *supra* note 130; and *Wilson*, *supra* note 130.

183 "Average privacy policy takes 10 minutes to read, research finds", *OUT-LAW News* (June 2008) online: <http://out-law.com/default.aspx?page=9490>.

184 See Kevin McLaughlin, "The Fourth Amendment and Cell Phone Location Tracking: Where Are We" (2007) 29 Hastings Comm. & Ent. L.J. 421 at 432; Information & Privacy Commissioner of Ontario, *Privacy by Design*, online: <http://www.privacybydesign.ca>.

combination of methods can be used as well to ensure the desired level of security. Increasingly, privacy by design is being recommended as a means by which companies can take steps, at the design stage, to incorporate privacy values and features into their products and services.[185] While privacy by design is not a complete or necessarily unproblematic solution to privacy concerns, technology can offer some options to consumers.

In the context of location-based services, privacy by design would mean that systems and processes are designed to only receive the information needed in order to efficiently process the user's request. Further, such processes may strip identifiers from information if these are not necessary to the process. In this way, a balance may be maintained between the needs of the location-based service provider and consumers' privacy interests.

(a) Existing solutions

Some companies embed privacy management tools within their devices and services. This allows individuals to manage their location data and to control the amount of information that is disclosed to third parties. For example, one can choose to only reveal general location information, such as country, or elect to divulge further details, such as city or street.[186] These measures are appropriate in certain contexts. For instance, a postal code is sufficient to provide the user with a list of Italian restaurants in the area. However, in many cases, in order to provide a truly interactive and practical service, the user would have to disclose more than just general location data.

Pseudonymization is a technique that has been employed to protect privacy. The user's location is associated with a pseudonym, rather than an actual name. However, this method proved to be flawed, as it quickly became evident that other identifying information such as the user's residence or workplace could easily be discerned with minimal background information about the user.[187] Alternatives to *pseudonymization* have been researched and advanced in the last few years. Their main goal is to find ways to protect the association between the user and her private information that could lead to re-identification.[188]

(b) Proposed Solutions

To respond to the threats posed by location-based services to mobile users' privacy, researchers have looked into mechanisms able to strip user's location data from any features that would reveal their identity.[189] Several studies have shown

---

185 FTC, *supra* note 56 at 40-41. See also: Ann Cavoukian, *Privacy by Design: The Seven Foundational Principles* (January 2011) online: <http://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf>.

186 Bellavista, *supra* note 35 at 88.

187 *Ibid.*

188 C. Bettini et al, "Anonymity and Historical Anonymity in Location-Based Services" 2009 LCNS 55991 at 3, online: <http://www.springerlink.com/content/t4t675126742/#section=185040&page=1>.

189 *Ibid.*

that the separation between a user's location data and her identification information can be achieved through technological data protection methods such as location anonymiser (*K-anonymiser* method), cryptographic techniques, obfuscation or others.

(i) K-anonymiser

Location anonymiser method, or *K-anonymiser*, aims to ensure that the location-based service, or an adversary that intercepts the communication between the mobile user and the location-based service, cannot link the location data with a specific user.[190] In order to frustrate any attempts to infer the exact location of a mobile user who placed the location-based query, a Location Anonymiser service, a trusted third-party, will generate a "cloaking region" to mask the user's location.[191] The Location Anonymiser service retains the current location of all its subscribed users. The cloaking region generated is then grouped with k number of requests from multiple users, and all these requests are sent to the location-based service to be processed at the same time.[192] The value of k can be adapted to guarantee anonymity.[193] Where there are not enough requests from users, dummy requests can be created to simulate additional users. The results generated by the location-based service are sent back to the Location Anonymiser service where they are filtered, and only the user's desired result is sent back to her.[194]

The k-anonymisation method entails sending the query to the service provider without any modifications. Where the query is for a highly specialized service, it might provide context that could in turn lead to the re-identification of the user.[195] Furthermore, if an adversary or the location-based service is aware of the value of k, inferences might be drawn and the mobile user can be re-identified through an elimination process.[196] An added concern is posed by the Location Anonymiser's ability to store a set of requests issued by each mobile user and the sequence of her location updates. This makes the private information stored on the trusted server vulnerable to correlating attacks. Because the anonymisation method relies on a trusted anonymiser system to function, this trusted system is a single point of at-

190 Shek, *supra* note 47 at 23.

191 Hasan et al, *supra* note 90 at 1.

192 See e.g. Shek, *supra* note 47 and Hasan et al, *supra* note 90.

193 For example, if user chooses in her options that k=5, the location anonymiser will forward to the location-based service the user's location and at least four more locations from other. This ensures that the user's location and her identity are not easily identifiable by the location-based service or an adversary.

194 Shek, *supra* note 47 at 23.

195 Hasan et al, *supra* note 90 at 1.

196 For example, if k=4, and the query is for a female hospital. If only one of the users sending this query to the location-based service is a female, it is a simple inference that it is that particular user who sent the query and re-identification is possible. For similar scenarios regarding the dangers of k-anonymisation method, see Hasan et al, *ibid* at 2. See also Bettini, "Protecting Privacy", *supra* note 90.

tack[197] that could potentially lead to exposure of private information of users.[198]

(ii) Cryptographic Techniques

Cryptographic techniques make use of data encryption in order to conceal information regarding a user's identity. For example, in place of a user's identity data being passed to the location-based service, a secure hash is sent along with the user's request. The location-based service will process the request without having access to the identifying information of the mobile user.[199] Because these cryptographic techniques make use of sophisticated computational and application codes, they are not yet suitable for use in low-powered mobile devices.

(iii) Obfuscation

Obfuscation is the process by which an individual can choose to degrade the quality of information being sent to the location-based service, in order to protect her privacy. The type of location information needed varies with different applications. For example, in order to receive current weather information, the application only needs to know the city or postal code where the mobile user is located.

There are two ways to achieve deliberate imperfection in spatial information: using *inaccuracies* or *imprecision*. Either one of these techniques can be used to achieve obfuscation of a mobile user's location.[200] When using *inaccuracies*, the location reported does not conform with reality, such as "X (the user) is in Quebec", when in fact, X is in Ontario. *Imprecisions* make use of real information but they do so in a way that makes it impossible to pinpoint the location with any precision. For example, "X is in Canada", is a true statement, but Canada is a large country. A statement such as "X is in Eastern Canada" is still vague and still cannot allow the location of X to be determined with any exactness, as there are no clear boundaries of Eastern Canada.[201]

Imprecision of location has been identified as one of the best methods to obfuscate the mobile user's location, as it presents a number of advantages. This approach reveals to the location-based service just enough information to furnish the desired response to the user. Obfuscation by *imprecision* is flexible and can be tailored to reveal the true location information with the desired degree of precision needed in specific contexts. This method allows for a direct connection between the mobile user and the location-based service, without the need for an intermediary, as is needed when using the k-anonymisation method.

---

197 Gabriel Ghinita et al, "Private Queries in Location-based Services: Anonymizers are not Necessary" Proceedings of the 2008 ACM SIGMOD international conference on Management of data, (ii), 121at 121, online: <http://portal.acm.org/citation.cfm?id=1376616.1376631>.

198 Hasan et al, *supra* note 90 at 1.

199 Shek, *supra* note 47 at 24.

200 See Matt Duckam et al, "A Formal Model of Obfuscation a Negotiation for Location Privacy" in *Pervasive Computing*, 2005 LNCS 3468152 at 156, online: <http://www.springerlink.com/content/kwlvm0de5mga8de2/fulltext.pdf>.

201 *Ibid* at 157.

(iv) Access Control

Privacy can also be ensured by traditional access control mechanisms triggered when certain conditions based on the user's physical location are satisfied. The user's physical location is securely verified to meet particular criteria, and access is granted to a service only when these criteria are met (e.g. user is in a specific zone, such as a shopping mall).[202] The access granted to the service can also be limited and controlled by privacy policies. For example, a user entering a large shopping center may only want to receive advertisements and coupons related to women's clothing. She can set her preferences on the mobile device and, upon entering the shopping center, only the desired types of advertisements are pushed to the mobile device.

CONCLUSION

The proliferation of location-enabled mobile devices in the hands of consumers has led to a rapid development of location-based services. The collection, use and disclosure of personal location information via these services raises serious privacy concerns, particularly given the sensitive nature of location information. While data protection laws may impose limits on the collection, use and disclosure of this information, there are gaps in the legislative framework, and in any event, a complaint-driven approach alone is not sufficient to ensure adequate protection of consumer privacy.

As with many other services delivered through wireless communications, there are significant issues around how the consent requirements of data protection legislation can be effectively met. The use of standard form contracts involving multiple links and complex privacy policies is not an effective method to give notice to consumers about the collection, use and disclosure of location information, particularly given its sensitive nature. Similarly, default settings may undermine privacy protection if they require consumers to opt into sharing by default. A business culture that values more restrained collection, use and disclosure of personal information, and shorter retention periods, will favour privacy protection and will also limit the potentially devastating impact of large scale data breaches. Limited collection and shorter retention periods will also reduce the scope of the impact of increased reliance on data in the hands of private sector companies by law enforcement officials.

It would be useful to see the development of guidelines, preferably in a cooperative manner between federal and provincial privacy commissioners that expressly address the appropriate norms for notice and consent to data collection in online and mobile environments. Such norms should consider requirements for repeated notifications where services are consumed on an ongoing basis for extended periods of time. More work needs to be done as well on best practices in the drafting of privacy policies that are accessible, easy to read, and ensure that consumers are given realistic opportunities to be informed of the nature of any information

---

202 C.A. Ardagna & M. Cremonini, "Access Control in Location-Based Services" in *Privacy in Location-based Applications*, C. Bettinii et al, eds, (Springer-Verlag Berlin Heidelberg, 2009) at 7-8, online: <http://spdp.dti.unimi.it/papers/Chapter5-ACDS.pdf>.

collection, and how their information will be used or disclosed by the service provider. Guidelines should also address the use of automated privacy settings.

Ultimately, more and better enforcement tools will also be required to allow the federal privacy commissioner to add weight to the development of norms in this area. The ability to name and shame data security breach notification requirements, order-making powers and the ability to impose significant fines on companies whose handling of personal information results in undue harm to consumers are all important ways to ensure compliance with privacy norms.

Although location-based services may offer attractive and beneficial opportunities to consumers, they do pose significant privacy risks. Because of the sensitive nature of location information, these risks may translate into significant material, moral and even physical harm. This is an area that calls for clear, proactive policy guidance and strong enforcement measures.